IN THE CLAIMS:

Please cancel claims 1-4 and 16-20 without prejudice or disclaimer, amend claim 5, and add new claims 21-28 as follows:

1-4. (Cancelled)

5. (Currently Amended) [[The]] A method for countering unauthorized decryption ~~according to Claim 1~~ comprising a step of scrambling at least one correlation between a data decryption processing in a hardware and at least one respective hardware operational phenomenon by randomly changing at least one arithmetic operation order in the data decryption processing, wherein the correlation is scrambled by an arithmetic operation method implemented by an information processing apparatus comprising the steps of:

for two integers K1 and K2, when finding a value F(K, A) of a function F satisfying F(K1+K2, A)=F(K1, A) ○ F(K2, A) (○ denotes an arithmetic operation in a communtative semigroup S. K designates an integer and A designates an element of S), decomposing the K to the sum of m integers K[0] + K[1] + ... K[m-1];

using T(0), T(1), ... T(m-1) resulted from rearranging a string of integers 0, 1, ...m-1 by permutation T; and

operating on terms F(K[T(0)], A) to F(K[T(m-1)], A) on the right side of F(K, A) = F(K[T(0)], A) ○F(K[T(1)], A) ○ ...F(K[T(m-1)], A) ... ("expression 1") in an order of F(K[T(0)], A), F(K[T(1)], A), ... F(K[T(m-1)], A) to find F(K, A).

6. (Original) The method according to claim 5, whereby the permutation processing, the permutation T prevents predicting any post-permutation data from pre-permutation data, or the permutation T is performed based on a dummy random number, and whereby the permutation processing is performed each time the expression 1 is performed.

7. (Original) The method according to claim 5, wherein the S is a commutative semigroup in which, for a set consisting of residues by an integer N ($N \geq 2$), the arithmetic operation ○ of a modular multiplication operation A○B=A*B mod N is

introduced, and the F satisfies F(K, A)=A^K mod N (A^K denotes the K-th power of A).

8. (Original) The method according to claim 5, wherein the information processing apparatus is installed on an IC card, a cellular phone, or a PDA.

9. (Original) The method according to claim 7, wherein the integer K is split in a form of $K[j] = u*((2^t)^j)$ $(0 \leq u \leq (2^t)-1, t = 1,2,....)$

10. (Original) The method according to claim 9, whereby the permutation processing, the permutation T is performed based on an information source prevents predicting any post-permutation data from pre-permutation data, or the permutation T is performed based on a dummy random number, and whereby the permutation processing is performed each time the expression 1 is performed.

11. (Original) The method according to claim 9, wherein the integer K is split in a form of $K[j] = u*((2^t)^j)$ $(0 \leq u \leq (2^t)-1, t = 1,2,....)$

12. (Original) The method according to claim 5, wherein the S is a Mordell-Weil group on an elliptic curve E defined on a finite field GF(p) (p is a prime number) or GF(2^n) (n is an integer equal to or greater than 1), and an expression F(K,A)=KA is satisfied, wherein the A denotes a point on the elliptic curve E, the KA denotes the arithmetic operation○ performed on K number of As such that the KA denotes A○A○A ...○A (K number) when the K is positive, or (-A)○(-A)○(-A)...○(-A) (|K| number) when the K is negative, and 0 (the point at infinity) on the E when the K is 0, the ○ denotes an addition operation in the Mordell-Weil group, and the -A is an inverse in the Mordell-Weil group of the A.

13. (Original) The method according to claim 12, wherein the information processing apparatus is installed on an IC card.

14. (Original) The method according to claim 12, wherein the integer K is split in a form of K[j] = u*((2^t)^j) ($0 \le u \le (2^t)-1$, t = 1,2,....)

15. (Original) The method according to claim 14, wherein the information processing apparatus is installed on an IC card.

16-20. (Cancelled)

21. (New) A method for calculating a value F(K, A) of a function F satisfying F(K1+K2, A) = F(K1, A) O F(K2, A) for two integers K1 and K2 in an encryption or decryption process of a cryptosystem by means of an information processing device which comprises a processing unit and a memory device, wherein O denotes an arithmetic operation in a commutative semigroup S, K designates an integer, and A designates an element of S, the method comprising:

decomposing the value K in the processing unit to m integers K[0], K[1], ..., K[m-1] each of which is a value of a n-bit unit of a binary representation of the value K, wherein the binary representation of the value K is w bit, m*n equals w; and

calculating F(K[T(0)]*(2^n)^(m-1-T[0]), A) O F(K[T(1)]*(2^n)^(m-1-T[1]),A) O, ... F(K[T(m-1)]*(2^n)^(m-1-T[m-1]), A) in the processing unit in an order of F(K[T(0])*(2^n)^(m-1-T[0]), A), F(K[T(1)]*(2^n)^(m-1-T[1]), A), ... F(K[T(m-1)*(2^n)^(m-1-T[m-1]), A) defined by a string of integers T(0), T(1), ...T(m-1) which is a random permutation of a string of integers 0, 1, ... m-1.

22. (New) The method according to claim 21, the permutation being performed based on a dummy random number each time the F(K[T(0)]*(2^n)^(m-1-T[0]), A) O F(K[T(1)]*(2^n)^(m-1-T[1]), A) O, ... F(K[T(m-1)]*(2^n)^(m-1-T[m-1]), A) is calculated.

23. (New) The method according to claim 21,

wherein the commutative semigroup S is a Mordell-Weil group on an elliptic curve E defined on a finite field GF(p) or GF(2^n),

wherein p is a prime number, n is an integer equal to or greater than 1, and an expression F(K,A)=KA is satisfied, and

wherein the value A denotes a point on the elliptic curve E, the value KA denotes the arithmetic operation O performed on K number of As such that the value KA denotes AOAOA ... OA when the value K is positive, or (-A)O(-A)O(-A) ...O(-A) when the value K is negative, or 0 on the elliptic curve E when the value K is 0, the symbol O denotes an addition operation in the Mordell-Weil group, and the value (-A) is an inverse in the Mordell-Weil group of the value A.

24. (New) The method according to claim 21, wherein the information processing device is an IC card.

25. (New) An information processing device for calculating a value F(K,A) of a function F satisfying F(K1+K2, A)=F(K1, A) O F(K2, A) for two integers K1 and K2 in an encryption or decryption process of a cryptosystem, wherein O denotes an arithmetic operation in a commutative semigroup S, K designates an integer, and A designates an element of S, the information processing device comprising:

a processing unit;

and

a memory device,

wherein the processing unit is adapted to decompose the value K to m integers K(0], K[1], ..., K[m-1], each of which is a value of a n-bit unit of a binary representation of the value K, wherein the binary representation of the value K is w bit, m*n equals w, and

the processing unit is further adapted to calculate

F(K[T(0)]*(2^n)^(m-1-T[0]), A) O F(K[T(1)*(2^n)^(m-1-T[1]), A) O,...

F(K[T(m-1)]*(2^n)^(m-1-T[m-1]), A) in an order of

F(K[T(0))*(2^n)^(m-1-T[0]), A), F(K[T(1)1*(2^n)^(m-1-T)[1], A), ...

F(K[T(m-1)]*(2^n)^(m-1-T[m-1]), A) defined by a string of integers T(0), T(1), ... T(m-1) which is a random permutation of a string of integers 0, 1, ... m-1.

26. (New) The information processing device according to claim 25, wherein the processing unit is adapted to perform the to permutation based on a dummy random number each time the F(K[T(0)]*(2^n)^(m-1-T[0]),A) O F(K[T(1)]*(2^n)^(m-1-

T[1]), A) O, ...
F(K[T(m-1)]*(2^n)^(m-1-T[m-1]), A) is calculated.

27. (New) The information processing device according to claim 25,

wherein the commutative semigroup S is a Mordell-Weil group on an elliptic curve E defined on a finite field GF(p) or GF(2^n),

wherein p is a prime number and n is an integer equal to or greater than 1, and an expression F(K,A)=KA is satisfied, and

wherein the value A denotes a point on the elliptic curve E, the value KA denotes the arithmetic operation O performed on K number of As such that the value KA denotes AOAOA ... OA when the value K is positive, or (-A)O(-A) O(-A) ... O(-A) when the value K is negative, or 0 on the elliptic curve E when the value K is 0, the symbol O denotes an addition operation in the Mordell-Weil group, and the value (-A) is an inverse in the Mordell-Weil 25 group of the value A.

28. (New) The information processing device according to claim 25, wherein the information processing device is an IC card.